Commanding in Multi-Domain Formations

Maj. Anthony M. Clas, EdD, U.S. Army

The general who wins the battle makes many calculations in his temple before the battle is fought. The general who loses makes but few calculations beforehand.

—Sun Tzu, *The Art of War*

T he three pillars of the U.S. Department of Defense strategy are *protect the homeland, build security globally,* and *project power and win decisively.*[1] The U.S. military presence around the world resulting from this strategy continues to provide its armed forces opportunities to bridge the gap into the future of warfare—war on a multi-domain battlefield. Multi-domain battle is the conceptual framework used to visualize potential combined arms capabilities across physical and psychological domains required against a near-peer enemy threat in an emerging twenty-first century multi-domain operational environment (MDOE).[2]

Key areas of consideration on the multi-domain battlefield are cultural, technological, and military attributes that shape the MDOE, ethical dilemmas created by emerging technologies including those caused by the fielding of disruptive technologies, the operational and strategic implications of dense urban environments on military objectives, and the roles of leaders and soldiers.

The purpose of this article's analysis is to develop a comprehensive picture of the arising needs of a future MDOE in order to orient readers to where further

research and shifts in approach ought to be directed. One of the underlying assumptions is the need for a collaborative approach between the United States, NATO countries, and partnered nations against potential adversarial threats. It is logical to visualize and prepare for combat operations against a near-peer enemy threat by 2050, given predictions of how the planet will change. For one, the United Nations predicts a population growth of 2.6 billion.[3] Additionally, climate change and biofuel use will triple by 2040, generating conflicts over land and water resources to keep up with the renewable energy demand.[4] As resources diminish and political tensions rise, military alternatives may be seen as more viable options as opposed to diplomatic solutions. Consequently, preparation via new research, new institutions, new methods for readiness, and new concepts for future conflict against a near-peer adversary must be developed now.
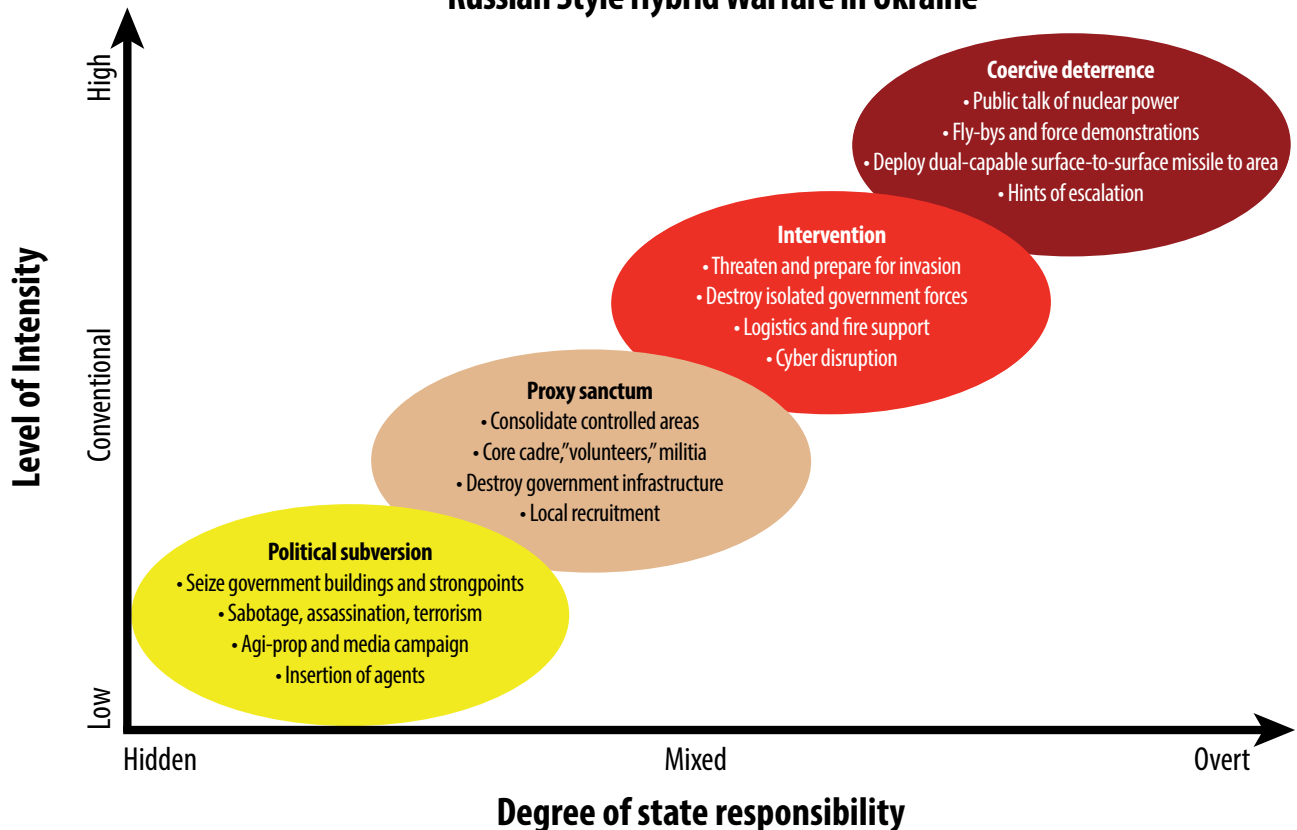
Attributes of Multi-Domain Battle in 2050

The MDOE will continue to generate new threats to U.S. national security. The United States may potentially maintain military primacy through 2050 due to continued globalization of military activities under the Unified Command Plan, which provides operational direction to U.S. armed forces and sustains a global military network in allied nations.[5] Nevertheless, it is naïve to believe that near-peer adversaries, state and nonstate actors alike, will not test the resolve of U.S. and NATO allies and partner nations. The attributes of a 2050 MDOE are being manifested in emerging capabilities now.

One of the primary attributes of the 2050 MDOE is emerging technologies and their relationship to the cultural norms of an interconnected world. Emerging technology will be designed to have less impact in the physical realm and more in the abstract cognitive domain. Minimum casualties and maximum gains via

Russian Style Hybrid Warfare in Ukraine

Coercive deterrence
- Public talk of nuclear power
- Fly-bys and force demonstrations
- Deploy dual-capable surface-to-surface missile to area
- Hints of escalation

Intervention
- Threaten and prepare for invasion
- Destroy isolated government forces
- Logistics and fire support
- Cyber disruption

Proxy sanctum
- Consolidate controlled areas
- Core cadre,"volunteers," militia
- Destroy government infrastructure
- Local recruitment

Political subversion
- Seize government buildings and strongpoints
- Sabotage, assassination, terrorism
- Agi-prop and media campaign
- Insertion of agents

Level of Intensity: High / Conventional / Low

Degree of state responsibility: Hidden / Mixed / Overt

(Graphic by Philip Karber)

Figure 1. Karber Hybrid Warfare Framework

influence and soft power in place of brute force will be the overarching theme given the current cultural milieu and emerging technology. Although population growth may recommend a more robust presence for security, network-centric warfare governed by political influence may be the key element of the MDOE in 2050.

Network-centric warfare. Network-centric warfare can be defined as effects-based operations that could permit a decentralized force to operate systematically as a dispersed mass.[6] Using smart munitions such as Global Positioning System-guided ballistic missiles against an enemy force is an example of network-centric operations on the battlefield. This concept also affords a psychological advantage over an adversarial force because a network-centric force will have the capability to concentrate fires precisely where desired.[7] This psychological advantage will leverage information operations designed to augment a larger diplomatic goal.

Noopolitics and the noosphere. Noopolitics is an international political leadership strategy combining the cyberspace network and mass media to manipulate the attitudes, opinions, or moral values of the general public.[8] In the noosphere, some observers assert, interoperability of cybertechnology and information operations within the information environment afford maximum payoff with minimal risk for state and nonstate actors. The two key elements of information warfare in this context are network-centric warfare and information operations that have a psychological impact.[9] A premier example of the future of information warfare can be seen in what Western thinkers term the emerging *hybrid warfare* campaign Russia is waging against the United States and its European allies in their escalating approach toward regional dominance.

Hybrid warfare. In eastern Europe, hybrid warfare—called "new-type warfare" by the Russians—is raising concerns in the United States as well as in other sovereign nations across Europe. Hybrid warfare is described as covert activities along with conventional and/or nuclear forces to influence domestic politics in targeted

countries.[10] Whether hybrid warfare is truly a military transformation is still to be determined. However, hybrid warfare appears to bridge the gap to a multi-domain battlefield. Figure 1 (on page 92) depicts the principles of hybrid-warfare actions measured by levels of intensity and degrees of state responsibility.[11] The complexities of an MDOE will require leaders and soldiers to find more innovative ways to achieve dominance over an adversary in the nuanced and complex arena of the noosphere.

Challenges and Ethical Dilemmas Created by Emerging Technology

Emerging technology continues to affect exponentially the evolution of warfare. For example, as we begin to normalize drone use in military operations, more emerging technologies are being developed in the forms of signal deconfliction for electronic warfare; alternative positioning, navigation, and timing for global positioning systems; artificial intelligence for cyberwarfare operations; and swarm and counterswarm nanotechnology—all of which will figure prominently in the 2050 MDOE.[12] The massive and rapid changes in technology, both in the military and civilian spheres, raises great difficulty for collective adjustment to the rule of law, at both the state and international levels.

Multi-domain battle is the result of advances in cyberwarfare, the use of unmanned aerial vehicles, and the use of artificial intelligence, which consequentially has raised concerns over violations of international law and the law of war.[13] The law of war construct results from the balance between contrasting interests of military necessity and humanitarian concerns.[14] As technology evolves and provides greater capabilities for both allies and adversaries, the more difficult applying the rule of law will be. International laws of warfare that apply to both "technologically-specific," a certain weapon system, and "technologically-neutral," a class of technology that can be weaponized—such as drones or artificial intelligence—and categorized by effect, may require a transformation of society for the governance of emerging technology.[15] Universal conscription and security sector governance are potential methods to stay within the lines of morality agreed upon within the social contract framed around civil-military relations.

Universal conscription. Universal conscription is one recommendation made to counter the dilemmas created by emerging technology. Modern technology affords militaries the capability to project combat power across the globe with minimum casualties.[16] Removing the human aspect from the battlefield further tips the balance in favor of military necessity, vice humanity, which is problematic when escalation of force includes a nuclear option. A conscript military will reflect society as a whole, vice an elite group of volunteers, and the conscripted service members will bring their experiences with the complexities of evolving technologies in the defense industry.[17] It is fair to assume emerging technology will play a vital role in combat scenarios as advances in nanotechnology, information, communication technology, and robotics come to fruition.[18] Universal conscription is a viable option in creating a vested interest by society to address moral concerns; however, there still needs to be a catalyst to generate a shared buy-in across the societal spectrum to build the technological capacity to compete in a future MDOE.

Security sector governance. The evolution of civil-military relations, otherwise known as the military's role in society, is transitioning to security sector governance, which strives for democratic oversight and accountability of security forces. Security sector governance is a holistic approach that empowers congress and the military, and also employs nongovernment organizations to include academic research institutes, professional organizations, media, and civilian experts that have the capability to provide assessments of and insights into national security issues.[19]

An example of this concept can be found in Harley-Davidson Motor Company's contribution of ninety thousand motorcycles for military use and the opening of the Harley-Davidson Quartermaster School to teach military mechanics motorcycle maintenance during the two world wars.[20] Security sector governance is the current trend amongst Western nations to manage the appropriate talent required to address the threats in the future

Maj. Anthony M. Clas, U.S. Army, is a public affairs officer in command of the 7th Mobile Public Affairs Detachment, Fort Hood, Texas. He holds a BA from Saint Xavier University, an MMAS from the U.S. Army Command and General Staff College, an MS from Tiffin University, and an EdD from Argosy University. His assignments include tours in Europe and deployments in support of Operations Iraqi Freedom and New Dawn.

MDOE. In terms of efficiency, it is much easier to recruit expertise and technology from industry than grow it in the military. Collaboration across society can be the catalyst for creating a sense of urgency to develop and equip the force with emerging technology and reduce capability shortfalls more rapidly.

Rapid fielding of emerging technology. The Army Rapid Capabilities Office is capable of fielding equipment within anywhere from one to five years depending on the level or echelon. However, the MDOE will not afford years to field capabilities to react to an adversarial force. Figure 2 (on page 95) depicts methodology the Army intends to use in Fiscal Year 2018 to create an "innovation ecosystem" leveraging industry partners to close capability gaps, which was introduced at the 2017 Association of the United States Army Annual Meeting and Exposition.[21] Equipment procurement falls victim to the adage that it can be developed fast, of high quality, or inexpensive, but it cannot possess all three characteristics. With current constraints driven by the U.S. economy on military expenditures, there is no simple solution to solve the fielding of weapons systems required for the MDOE.[22]

Prototyping methodology is one feasible option to rapidly field emerging technology to provide the required capability to the force when an adversary poses a threat. Prototyping methodology consists of identifying capability shortfalls, defining the problem, deconstructing the problem, and defining solution options, and then developing and assessing a prototype. The output is a "put-on-the-shelf" strategy acquisition process that would be more in line with how conflict will develop in the future.[23] By assembling prototype housing offices in the future, creativity and innovation can be applied to create options that can be used against potential adversaries. However, there are certain conditions that must be met to ensure reaping the benefits of the prototyping process:

- Results are used to inform key program decisions.
- The prototype is designed to demonstrate the critical attributes of the final product in a realistic environment.
- Prototyping strategies and documentation are austere.
- There should be no commitment to production during the prototyping phase.
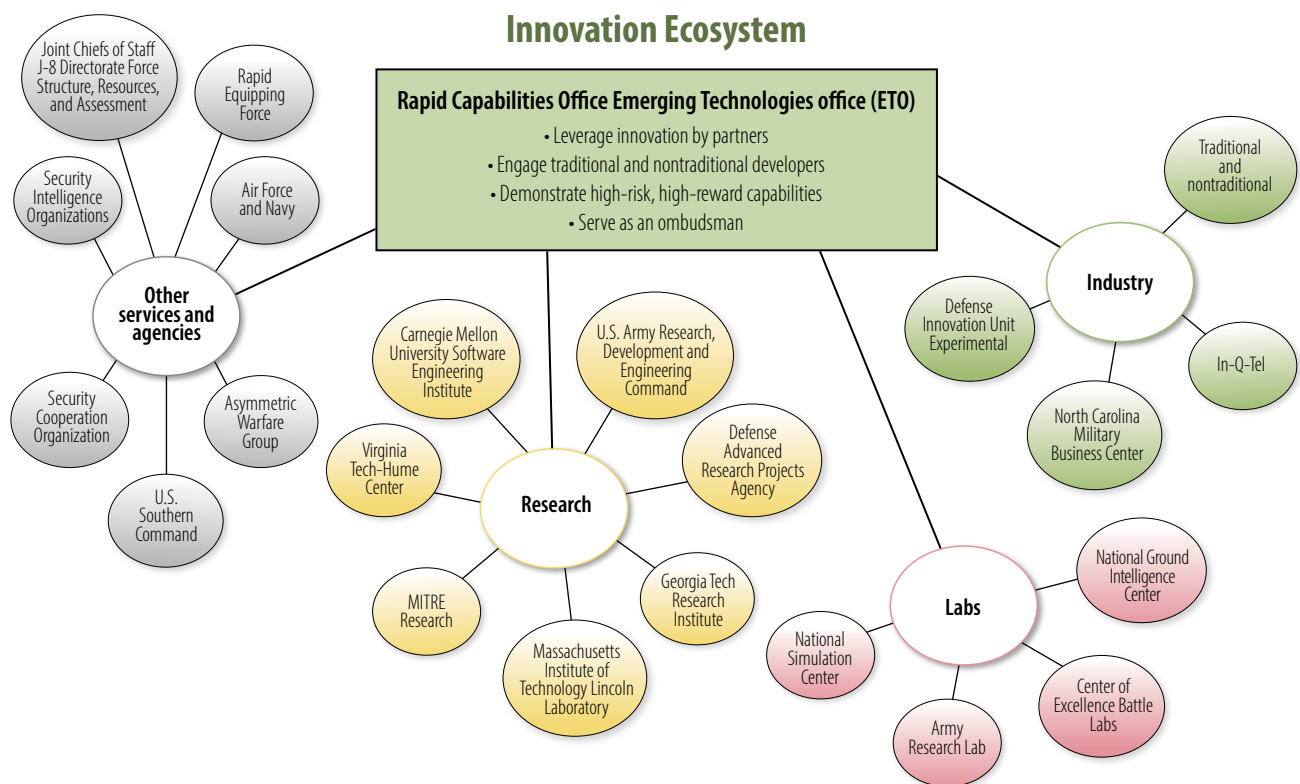- No additional requirements are added or performance increases expected.[24]

If the stakeholder does not ensure the aforementioned conditions are met the prototyping process could end up more costly and less timely fielding the required technology. If the conditions are set correctly, the prototyping process should cut down the acquisition cycle from years to months, thereby reducing costs applied to fielding equipment that will be obsolete by the time it is implemented against an adversary in an MDOE.[25] Innovation and speed will be of the utmost importance as we move to more urban operational environments, such as megacities, due to an escalating world population resulting in dense urban environments.

Impacts of Dense Urban Environments

Megacities are complex operating environments that pose significant challenges on military forces. Two primary concerns in this environment are minimizing collateral damage to noncombatants and preserving infrastructure to mitigate the suffering of the local populace.[26] Due to dense populations growing at alarming rates and infrastructure that significantly reduces effective intelligence, surveillance, and reconnaissance operations, adversaries may select dense urban environments to establish a base of operations. Developing a strategy that shapes the civil capacity of the infrastructure in concert with information operations that focus on the abstract and cognitive domains continues to need development of strategy, technology, and planning to deter civil unrest and reduce an adversary's advantage in an MDOE.

On the strategic level, using security-sector reform procedures and institutions to shape the economic and information environments to create a "smart city"—one that uses technology and the information environment to efficiently manage resources—may be a worthy strategy to strengthen social quality and reduce social exclusion, which leads to highly restrictive multi-domain battlefields. The elements of a smart city required to improve social quality are social and economic security, social cohesion, and social inclusion.[27]

Even with effective target discrimination, a kinetic fight in dense urban terrain has a high probability of resulting in collateral damage that will benefit an adversary in the information environment. Findings from certain Army megacity experimentation exercises (called Unified Quest) identified a need for strong information operations, the value of special operations forces

Innovation Ecosystem

Rapid Capabilities Office Emerging Technologies office (ETO)
- Leverage innovation by partners
- Engage traditional and nontraditional developers
- Demonstrate high-risk, high-reward capabilities
- Serve as an ombudsman

Joint Chiefs of Staff J-8 Directorate Force Structure, Resources, and Assessment

Rapid Equipping Force

Security Intelligence Organizations

Air Force and Navy

Other services and agencies

Security Cooperation Organization

Asymmetric Warfare Group

U.S. Southern Command

Traditional and nontraditional

Industry

Defense Innovation Unit Experimental

In-Q-Tel

North Carolina Military Business Center

Carnegie Mellon University Software Engineering Institute

U.S. Army Research, Development and Engineering Command

Defense Advanced Research Projects Agency

Virginia Tech-Hume Center

Research

MITRE Research

Georgia Tech Research Institute

Massachusetts Institute of Technology Lincoln Laboratory

National Ground Intelligence Center

Labs

National Simulation Center

Center of Excellence Battle Labs

Army Research Lab

(Graphic courtesy of the Army Rapid Capabilities Office)

Figure 2. The Army Rapid Capabilities Office (RCO) Acquisition Industry Link: RCO Emerging Technologies Office

and indigenous allies, limitations on the use of precision strike weapons designed for open warfare, and the requirement to incorporate stability activities throughout all phases of combat operations.[28]

Loss of life and significant damage to infrastructure reduces the resolve of the host-nation populace affected by a conflict, which will ultimately result in loss of support across the alliance to continue the fight. Confucius's philosophy pertaining to societies with dense populations applies here: "The quality of the population is more important than the quality of your armaments."[29]

Roles of Leaders and Soldiers in a Multi-Domain Battlefield

Gen. Mark Milley, chief of staff of the U.S. Army, suggests the military will require more mature and seasoned leaders to conduct ground combat operations in the future.[30] The ability of the United States to conduct combined operations with NATO allies

and partners is critical for facing future threats in an MDOE. Furthermore, a future MDOE will require leaders to be more innovative and agile when working through complex issues in combat.

Complex interdependence. The overarching theme relevant to leaders and soldiers alike in an MDOE is complex interdependence. Complex interdependence theory is defined as a mutual dependence between transnational actors due to growing ties that make each one vulnerable to each other's actions.[31] U.S. armed forces conducting combined exercises with ally and partner nations is a demonstration of complex interdependence, as countries work together to achieve interoperability between network-centric systems and increased situational understanding of each other's tactics and procedures. Innovative leaders in concert with complex interdependency is the best combination to develop a force prepared to operate in the future MDOE.

Soldiers from Company C, 1st Battalion, 68th Armored Regiment, 3rd Armored Brigade Combat Team, 4th Infantry Division, train with Estonian Defence Forces 23 March 2017 during Operation Golden Shovel on Kukepalu Range in Estonia. Operation Golden Shovel, a company-level combined training exercise under Operation Atlantic Resolve, gives U.S. soldiers a chance to understand how their Estonian counterparts respond to an armored attack, while Estonian soldiers gain a deeper understanding of U.S. techniques and tactics. (Photo by Staff Sgt. Charlene Moler, 7th Mobile Public Affairs Detachment, U.S. Army)

Entrepreneurial leadership. Entrepreneurial leadership is the concept of influencing and directing performance of an organization's members to identify and capitalize on new opportunities.[32] An evolving MDOE will require leaders and soldiers to exercise innovation when working through the complexities of a multi-domain battlefield. Entrepreneurial leadership involves three key tasks to be successful in military culture:

1. identifying the assumptions of the role of the ideal combatant that underlie an innovation, and the extent to which those new concepts align with the existing culture;

2. demonstrating the new assumptions that are misaligned with the prevailing culture to improve the organization's performance in the kinds of conflicts it anticipates; and

3. persuading the organization that the new concept of a combatant is not a rejection of the enduring values of the organization.[33]

In short, entrepreneurial leadership requires leaders to rapidly work through the observe-orient-decide-act (OODA) loop and mitigate groupthink which may hinder cultural change.[34] Operations that allow the

United States, its NATO allies, and partner nations the ability to practice deploying force packages forward using a holistic approach to conduct combined training exercises during peacetime will significantly increase readiness for future conflicts.

Lt. Gen. Ben Hodges, then commander of U.S. Army Europe, captures the OODA loop cycle in terms of "speed of recognition, speed of decision, speed of assembly, and finally, ready to fight tonight," as well as demonstrating complex interdependence with regionally allocated force (RAF) units operating in Atlantic Resolve and NATO's multinational enhanced forward presence battle groups

Information environment (inform)

Diplomacy	Complex interdependence →	Strong alliance
Informational	Network centric and mass-media operations →	Credibility preservation
Military	Mission command element →	Combined interoperability
Economics	Smart city →	Strong economy

Information environment (influence)
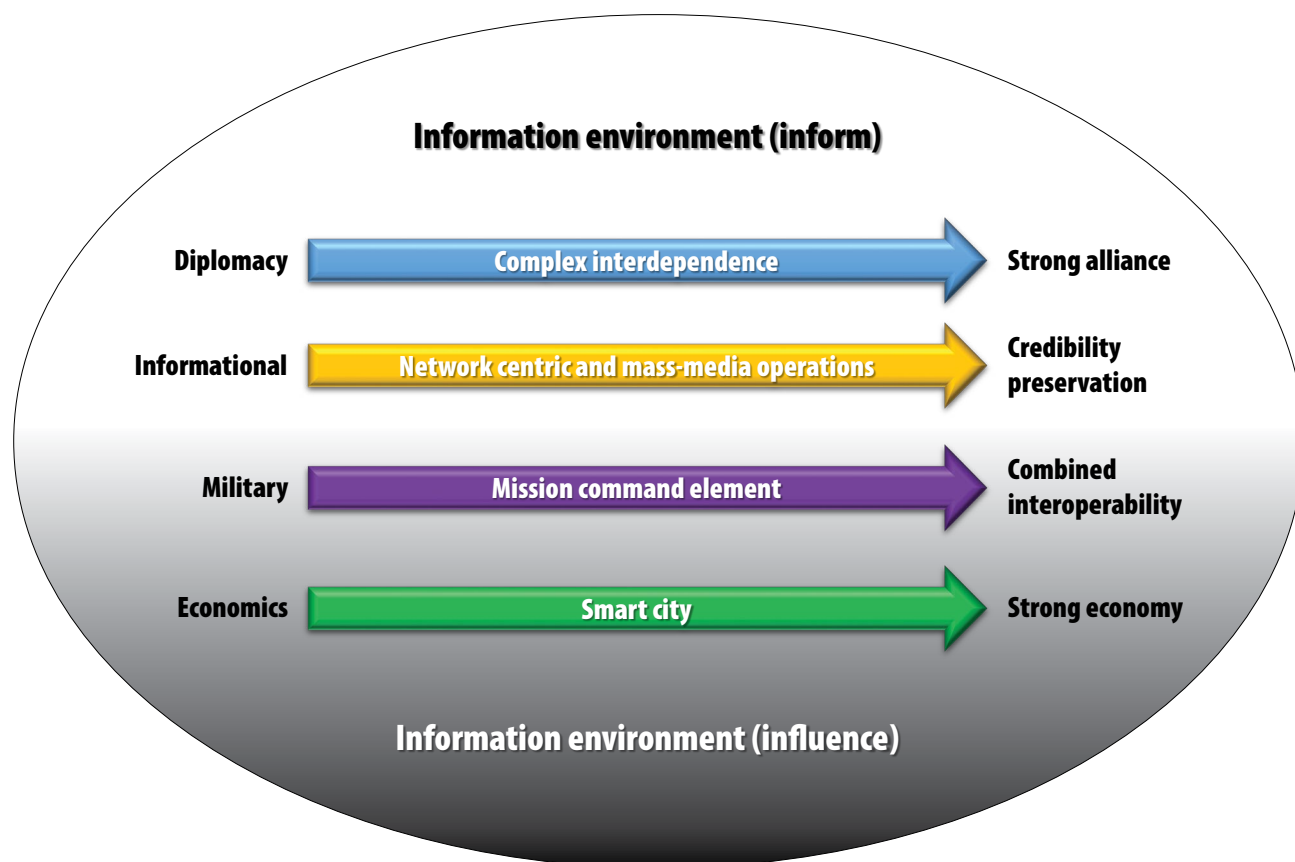
(Graphic by author)

Figure 3. Whole-of-Society Strategy for Multi-Domain Battle

conducting combined security operations in Poland, Estonia, Latvia, and Lithuania.[35] Continuing to develop complex interdependence with our NATO allies and partners in concert with empowering junior leaders to be innovative using entrepreneurial leadership is recommended to meet the "ready to fight tonight" immediacy in an MDOE. Gen. David Goldfein, chief of staff of the U.S. Air Force, proclaims the need for leaders to "visualize the multiple battlespaces and execute rapid decision-making" supporting an entrepreneurial leadership approach to react more decisively in an MDOE.[36]

European Reassurance Initiative and the Mission Command Element— Atlantic Resolve

The United States and other NATO countries are in the early stages of shaping the MDOE against future potential near-peer adversaries. The European Reassurance Initiative (ERI) is at the forefront of evolving Western

collective preparedness for a multi-domain battlefield. ERI provides funding to U.S. military forces and NATO allies and partners in an effort to collectively build deterrence capabilities against external threats or destabilization actions in the eastern European region.[37] Russia has committed several territorial and treaty violations in the region to include the illegal annexation of Crimea and aggression in eastern Ukraine, as well as violating the U.S.-Russia Intermediate-Range Nuclear Forces Treaty.[38] The U.S. and NATO response to the aforementioned violations was the deployment of forces to the eastern European region to initiate Atlantic Resolve, where U.S. and NATO allies and partners conduct multinational training and security cooperation activities using ERI fund allocations.[39]

The United States and NATO provide a good example of complex interdependence in the U.S. European Command, U.S. Army Europe-led Atlantic Resolve mission. The mission command element (MCE) for

Atlantic Resolve (MCE-AR) is a tactical division-level headquarters responsible for RAF units deployed in support of Atlantic Resolve in eastern Europe. The RAF units are operationally controlled by U.S. Army Europe and include a division-level MCE, an armored brigade combat team, a combat aviation brigade, and a combat sustainment support battalion serving as a rotational logistics force.[40] The MCE concept provides armed forces a forward element to streamline the OODA loop process in areas of potential future conflict and also incorporates elements of complex interdependence and entrepreneurial leadership.

Atlantic Resolve serves as a catalyst for preparing U.S. and NATO allies and partners for the threats they may face in an MDOE. The mission command model encompasses centralized planning for decentralized execution exercising disciplined initiative and adaptive leadership to maximize an element's effect in the MDOE.[41] The MCE concept affords NATO allies and partners the ability to synchronize efforts against network-centric proxy warfare, as well as a means to search for indicators and warnings that may trigger additional force requirements in the operational environment in a unified response.

Whole-of-Society and Strong Alliance

Russia's vigilance and use of hybrid warfare to build upon destabilization actions in eastern Europe affords U.S. and NATO allies and partners an opportunity to evaluate a whole-of-society (WoS) approach in an MDOE to create and maintain a strong alliance. Even though China may be a logical front-runner to surpass the United States economically by 2050 or sooner due to their rate of economic growth, the balance of power can shift more rapidly if a Sino-Russian alliance is formed.[42] A WoS approach encompasses a wide range of societal actors, to include all nations that comprise the NATO alliance.[43] Using the MCE-AR as a catalyst to strengthen the alliance between NATO allies and partner nations with a WoS approach will help counter emerging threats in the MDOE of the future.

Recommendations

Multi-domain battle is a complex issue that will continue to require attention as near-peer adversaries continue to revolutionize their tactics and capabilities.

The following recommendations are offered to better prepare the U.S. armed forces capturing themes of interdependence, interoperability, and societal inclusion against potential threats in an MDOE:

Strong alliance. Generate more opportunities to build complex interdependency between allied and partnered nations and create leadership development opportunities to apply entrepreneurial leadership using creativity and innovation to work through problem sets within the organization. Conducting a mixed-methods program evaluation to assess the MCE-AR's effectiveness in countering hybrid warfare on a multi-domain battlefield may determine if combining a WoS approach with the MCE concept is an effective strategy against future MDOE adversaries.[44]

Multi-domain battle. Hybrid warfare is just the beginning of network-centric proxy warfare. Noopolitics operating within the noosphere, cyberspace network, and mass media will become more prevalent as interconnectivity becomes more prevalent in cyberspace. Developing an emerging technology strategy tailored around the Unified Quest findings: strong information operations capabilities that bolster special operations forces' and indigenous allied forces' effects in an MDOE.[45] Implementing the "put-on-the-shelf" strategy by way of developing prototype housing offices can potentially significantly cut down on the acquisition process to get the right equipment to the military at the right time.

Enhanced civil-military relationships. Bolstering civil-military relationships via security sector governance and universal conscription may generate shared buy-in, minimizing ethical constraints and building essential emerging technology capabilities to defend against potential near-peer adversaries in the future MDOE.[46] It is uncertain if future near-peer adversaries will be Russia, China, or a combination presented as a Sino-Russia alliance. Consequentially, exploring WoS options to bolster social inclusion by incorporating security sector governance and universal conscription merit further inquiry. Figure 3 (on page 97) depicts a recommended WoS strategy using the four elements of national power: diplomacy, informational, military, and economic application to a future MDOE.[47]

Conclusion

The following areas are key focus points to narrow the gap in research and better prepare for

multi-domain battle: attributes that shape the multi-domain battlefield, roles of leaders and soldiers, ethical dilemmas created by emerging technologies, fielding of disruptive technologies, and the operational and strategic implications that dense urban environments have on military objectives. Although generalizability and validity are limited in this research, there were still several significant concepts worthy of future research.

Strong alliance, multi-domain battle, and smart city theory are concepts recommended for further evaluation to incorporate into a WoS strategy against the aforementioned focus areas in a future MDOE. The U.S. military needs to keep abreast of research and strategic effort in areas once considered outside of their lanes. Focus on technology development alone

can no longer suffice, given what is understood today about the 2050 MDOE. The future is uncertain, and all of the research we conduct will remain conceptual until our assumptions become reality. Until then, the best course of action is to continue the search for more efficient and creative methods to defend against future threats posed by near-peer adversaries on a multi-domain battlefield. ■

Disclaimer: The views and opinions expressed or implied in this research project are those of the author and should not be construed as carrying the official sanction of NATO, Department of Defense, U.S. Army, or other agencies or departments of the U.S. government or allied and partnered nations. This article may be reproduced in whole or in part without permission.

Notes

Epigraph. Lionel Giles, *Sun Tzu: The Art of War* (Blacksburg, VA: Thrifty Books, 2009), 3.

1. Department of Defense (DOD), *Quadrennial Defense Review* (Washington, DC: DOD, March 2014), v, accessed 27 October 2017, http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf.
2. DOD, "Multi-Domain Battle: Combined Arms for the 21st Century," United States Army-Marine Corps white paper (Washington, DC: DOD, January 2017), 2–6.
3. "World Population to Increase by 2.6 Billion over Next 45 Years, With All Growth Occurring In Less Developed Regions," United Nations press release, 24 February 2005, accessed 30 October 2017, https://www.un.org/press/en/2005/pop918.doc.htm.
4. Kent Randolph, "The Future of Warfare: Are We Ready?," *International Review of the Red Cross* 97, no. 900 (December 2015): 1347.
5. DOD, *Quadrennial Defense Review* (Washington, DC: DOD, March 2014), 63, accessed 30 October 2017, http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf.
6. Paul T. Mitchell, *Network Centric Warfare: Coalition Operations in the Age of US Military Primacy* (New York: Routledge, 2007), 12.
7. Paul Murdock, "Principles of War on the Network-Centric Battlefield: Mass and Economy of Force," *Parameters* 32, no. 1 (Spring 2002): 91.
8. Ibid., 92.
9. Nikolai Sergeevich Labush et al., "War and Armed Conflict in the Information Space," *International Review of Management and Marketing* 5, no. 1S (2015): 31.
10. Ibid., 32.
11. Andrew Radin, *Hybrid Warfare in the Baltics: Threats and Potential Responses* (Santa Monica, CA: RAND Corporation, 2017), 5. A detailed discussion of "new-type" warfare can be

found in Timothy Thomas, "The Evolving Nature of Russia's Way of War," *Military Review* 97, no. 4 (July-August 2017): 34–42; and in Valery Gerasimov, "Contemporary Warfare and Current Issues for the Defense of the Country," trans. Harold Orenstein, *Military Review* 97, no. 6, (November-December 2017): 22–27. Figure 1 reprinted with permission of Dr. Phillip A. Karber, "Coming to a Theatre Near You—Russia's New Generation Warfare" (lecture, U.S. Army Training and Doctrine Command, Fort Eustis, VA, 14 December 2015).
12. Phillip A. Karber, "The Russian Military Forum: Russia's Hybrid War Campaign: Implications for Ukraine and Beyond," The Center for Strategic International Studies and the Potomac Foundation (website), 10 March 2015, accessed 24 March 2017, https://www.csis.org/events/russian-military-forum-russias-hybrid-war-campaign-implications-ukraine-and-beyond.
13. Rain Livoja, "Technological Change and the Evolution of the Law of War," *International Review of the Red Cross* 97, no. 900 (December 2015): 1158.
14. Ibid., 1162.
15. Ibid., 1169.
16. Brad Allenby and Mark Hagerott, "Universal Conscription as Technology Policy," *Issues in Science and Technology* XXX, no. 2 (Winter 2014): 44.
17. Ibid., 46.
18. Ibid., 42.
19. Alexandre Lambert, "From Civil-Military Relations towards Security Sector Governance," *European Political Science* 10, no. 2 (June 2011): 161.
20. Mark Melief, Tycen Bundgaard, and Jordan Hathaway, "Strategic Report for Harley-Davidson," Pandora Group: Out of the Box Consulting, April 2006, 6, accessed 28 December 2017, http://economics-files.pomona.edu/jlikens/SeniorSeminars/pandora/reports/harley.pdf.
21. Doug Wiltsie, "AUSA Open Door," U.S. Army Rapid Capabilities Office (website), 11 October 2017, 5, accessed 7

December 2017, http://rapidcapabilitiesoffice.army.mil/_assets/downloads/Army_RCO_AUSA_Open_Door.pdf.

22. Richard Hencke, "Prototyping: Increasing the Pace of Innovation," Defense AT&L report (Fort Belvoir, VA: Defense Acquisition University, July-August 2014), 12, accessed 31 October 2017, http://www.dtic.mil/get-tr-doc/pdf?AD=ADA608683.

23. Jeffrey Dezner and Melinda Huang, "On Prototyping," RAND National Defense Research Institute Occasional Paper (Santa Monica, CA: RAND Corporation, 2009), 20, accessed 12 December 2009, https://www.rand.org/content/dam/rand/pubs/occasional_papers/2010/RAND_OP267.pdf.

24. Ibid., 14.

25. Ibid.

26. William G. Adamson, "Megacities and the US Army," Parameters 45, no. 1 (Spring 2015): 47.

27. Sergey A. Makushkin et al., "Role of Inclusion 'Smart City' Concept as a Factor in Improving the Socio-Economic Performance of the Territory," International Journal of Economics and Financial Issues 6, no. 1 (2016): 155.

28. Adamson, "Megacities and the US Army," 48.

29. Zhang Youmin and Li Tianchen, "Economic Lessons from Confucius for the New Century," Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies 4, no. 1 (Queensland, Australia: Bond University): 2, accessed 31 October 2017, http://epublications.bond.edu.au/cm/vol4/iss1/3.

30. Meghann Myers, "Milley: Future Conflicts Will Require Smaller Army Units, More Mature Soldiers," Army Times, 21 March 2017, accessed 31 October 2017, https://www.armytimes.com/articles/milley-future-conflicts-will-require-smaller-army-units-more-mature-soldiers.

31. Waheeda Rana, "Theory of Complex Interdependence: A Comparative Analysis of Realist and Neoliberal Thoughts," International Journal of Business and Social Science 6 (February 2015): 291.

32. Mozhdeh Mokhber et al., "Impact of Entrepreneurial Leadership on Organization Demand for Innovation: Moderating Role of Employees' Innovative Self-Efficacy," International Review of Management and Marketing 6, no. 3 (2016): 418.

33. Andrew Hill, "Culture and the US Army: Military Innovation and Military Culture," Parameters 45, no. 1 (Spring 2015): 94.

34. Michael W. Benitez, "Twenty-First-Century Air Warfare and the Invisible War: Strategic Agility," Air & Space Power Journal 29, no. 5 (September 2015): 86.

35. Ben Hodges, "Lt. Gen. Ben Hodges: US Army Europe and Its Role in Deterrence," Defense News, 5 December 2016, accessed 31 October 2017, http://www.defensenews.com/articles/lt-gen-ben-hodges-us-army-europe-and-its-role-in-deterrence.

36. David L. Goldfein, Chief of Staff of the Air Force, Letter to Airmen, "Enhancing Multi-Domain Command and Control: Tying It All Together," March 2017, accessed 31 October 2017, http://www.af.mil/Portals/1/documents/csaf/letter3/Enhancing_Multi-domain_CommandControl.pdf.

37. Office of the Under Secretary of Defense (Comptroller), "European Reassurance Initiative: Department of Defense Budget, Fiscal Year (FY) 2016" (Washington, DC: DOD, February 2015), 2, accessed 31 October 2017, http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2016/FY2016_ERI_J-Book.pdf.

38. DOD, "Operation Atlantic Resolve (2014) Fact Sheet," U.S. European Command Communication and Engagement Directorate, 29 January 2015, 1, accessed 12 December 2017, https://www.defense.gov/Portals/1/features/2014/0514_atlanticresolve/Operation_Atlantic_Resolve_Fact_Sheet_2014.pdf.

39. Ibid., 2.

40. Richard Sokolsky, "The New NATO-Russia Military Balance: Implications for European Security," task force white paper, Carnegie Endowment for International Peace (website), 13 March 2017, accessed 31 October 2017, http://carnegieendowment.org/2017/03/13/new-nato-russia-military-balance-implications-for-european-security-pub-68222.

41. U.S. Army Europe, "Atlantic Resolve Fact Sheet," U.S. Army Europe (website), 20 September 2017, accessed 31 October 2017, http://www.eur.army.mil/organization/factsheets/default.htm#operations.

42. Erich Weede, "Geopolitics, Institutions, and Economics: On the Rise and Decline of Civilizations," Geopolitics, History, and International Relations 8, no. 1 (2016): 178.

43. Jonathan Glennie and Gideon Rabbinowitz, "Localising Aid: A Whole of Society Approach" (report, London: Centre for Aid and Public Expenditure, June 2013), 11, accessed 31 October 2017, https://www.odi.org/publications/7571-localising-aid-whole-society-approach.

44. For a comprehensive overview of mixed-methods assessment methodology, see Patricia Burch and Carolyn J. Heinrich, Mixed Methods for Policy Research and Program Evaluation (Los Angeles: Sage Publications, 2016), 19.

45. Adamson, "Megacities and the US Army," 48.

46. Lambert, "From Civil-Military Relations towards Security Sector Governance," 161.

47. Brett D. Shehadey, "Putting the 'D' and 'I' back in DIME," In Homeland Security (website), 27 October 2013, accessed 31 October 2017, http://inhomelandsecurity.com/putting-the-d-and-i-back-in-dime/. The acronym DIME stands for diplomatic, informational, military, and economic.